On Kronecker-Trager's Factorization Method(Theory and applications in computer algebra)

AUTHOR(S):

片町, 健太郎; 椎原, 浩輔; 佐々木, 建昭

数理解析研究所講究録
第846巻 1993年 6-12

On Kronecker-Trager's Factorization Method

筑波大学大学院数学研究科　片町 健太郎 (Kentaro KATAMACHI)[1)]
筑波大学自然学類　椎原 浩輔 (Kousuke SHIIHARA)[2)]
筑波大学数学系　佐々木 建昭 (Takeaki SASAKI)[3)]

代数拡大体上の標準的な因数分解法としてはWeinberger-Rothchildのアルゴリズムが有名だが、Kronecker-Tragerのアルゴリズムも簡単で捨てがたい。本稿では、有理数体$\mathbb{Q}$に複数個の代数的数$\alpha_1,\cdots,\alpha_n$を添加する場合を扱う。従来はこのような場合でも1個の原始元に帰着させるのが常道であったが、$\alpha_1,\cdots,\alpha_n$の定義多項式がそれぞれ$\mathbb{Q}$上の多項式である場合には、Kronecker-Trager法を使うと効率的な計算が可能になることを示す。

1. 記法

$\mathbb{Q}$ ： 有理数体。

$\alpha_1,\cdots,\alpha_n$ ： $\mathbb{Q}$上代数的な数。
ただし、$\alpha_i \notin \mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1},\alpha_{i+1},\cdots,\alpha_n)$, $i=1,\cdots,n$, と仮定する。

$\mathrm{D}_i(t)$ ： α_iの$\mathbb{Q}$上の定義多項式 ($\mathbb{Q}$上で既約とする)。

${\alpha_i}^{(1)},\cdots,{\alpha_i}^{(m_i)}$、ただし, $m_i \stackrel{\mathrm{def}}{=} \deg(\mathrm{D}_i)$ ： D_iの各根。

$\mathrm{N}_{\alpha_i}(f)$ ： α_iに関するfのノルム (fは$\mathbb{Q}(\alpha_i)$上の多項式)。

$$\underset{\alpha_i}{\mathrm{N}}(f) \stackrel{\mathrm{def}}{=} \prod_{j=1}^{m_i} f(x,{\alpha_i}^{(j)}) = \mathrm{res}_t(f(x,t),D_i(t)),$$

$$\underset{\alpha_1,\cdots,\alpha_n}{\mathrm{N}}(f) \stackrel{\mathrm{def}}{=} \underset{\alpha_1}{\mathrm{N}}(\cdots(\underset{\alpha_n}{\mathrm{N}}(f))\cdots).$$

2. 基礎となる定理

本章に述べる定理はα_iの定義多項式D_iが$\mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})$上の多項式であっても成立する。

[1)] katamati@math.tsukuba.ac.jp
[2)] ks@math.tsukuba.ac.jp
[3)] sasaki@math.tsukuba.ac.jp

補題 1
$\alpha_i \notin \mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})$ とし、$f \in \mathbb{Q}(\alpha_1,\cdots,\alpha_i)[x]$ とする。f が $\mathbb{Q}(\alpha_1,\cdots,\alpha_i)$ 上既約ならば、$\mathrm{N}_{\alpha_i}(f)$ は $\mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})$ 上既約な多項式のべき乗となる。

証明
$\mathrm{N}_{\alpha_i}(f(x,\alpha_1,\cdots,\alpha_i))$ が $\mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})$ 上の互いに素な多項式 A と B に因数分解されたとする。

$$\underset{\alpha_i}{\mathrm{N}}(f) = A\cdot B, \quad \gcd(A,B) = 1.$$

$f_j = f(x,\alpha_1,\cdots,\alpha_i^{(j)})$ とおけば、f_1 は $\mathrm{N}_{\alpha_i}(f)$ の因子だが、既約なので A と B のどちらか一方、例えば A のみを割る (即ち、$A = f_1\cdot g_1$)。すると、拡大体の一般論により、$\mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})$ の要素を変えずに $\mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})(\alpha_i^{(1)})$ を $\mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})(\alpha_i^{(j)})$ に写す同型写像が存在する。この同型写像によって $A = f_j\cdot g_j$ が得られる。従って A は

$$f_1\cdots f_{m_i} = \underset{\alpha_i}{\mathrm{N}}(f)$$

の倍数となり、$\deg(B) = 0$ でなければならない。

定理 1
$\alpha_i \notin \mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1},\alpha_{i+1},\cdots,\alpha_n)$, $i = 1,\cdots,n$, とし、$f \in \mathbb{Q}(\alpha_1,\cdots,\alpha_n)[x]$ とする。f が $\mathbb{Q}(\alpha_1,\cdots,\alpha_n)$ 上既約ならば、$\mathrm{N}_{\alpha_1,\cdots,\alpha_n}(f)$ は $\mathbb{Q}$ 上既約な多項式のべき乗となる。

証明
補題 1 より、$j = n, n-1,\cdots,1$ に対し、$h_j(x,\alpha_1,\cdots,\alpha_{j-1})$ を $\mathbb{Q}(\alpha_1,\cdots,\alpha_{j-1})$ 上既約な多項式として、

$$\begin{cases} \mathrm{N}_{\alpha_n}(f) = h_n(x,\alpha_1,\cdots,\alpha_{n-1})^{k_n} \\ \mathrm{N}_{\alpha_{n-1}}(h_n) = h_{n-1}(x,\alpha_1,\cdots,\alpha_{n-2})^{k_{n-1}} \\ \quad\vdots \\ \mathrm{N}_{\alpha_1}(h_2) = h_1(x)^{k_1} \end{cases}$$

と表すことができる。したがって、$\mathrm{N}_{\alpha_1,\cdots,\alpha_n}(f)$ は以下のように書きかえることができる。

$$\begin{aligned} \underset{\alpha_1,\cdots,\alpha_n}{\mathrm{N}}(f) &= \underset{\alpha_1,\cdots,\alpha_{n-1}}{\mathrm{N}}\left(\underset{\alpha_n}{\mathrm{N}}(f)\right) \\ &= \underset{\alpha_1,\cdots,\alpha_{n-1}}{\mathrm{N}}\left(h_n{}^{k_n}\right) \\ &= \left(\underset{\alpha_1,\cdots,\alpha_{n-1}}{\mathrm{N}}(h_n)\right)^{k_n} \\ &= \cdots \\ &= h_1{}^{k_1\cdots k_n} \end{aligned}$$

即ち、定理が示された。

定理 2
$f \in \mathbb{Q}(\alpha_1, \cdots, \alpha_n)[x]$ とする。$\mathrm{N}_{\alpha_1,\cdots,\alpha_n}(f)$ が無平方ならば、$\mathrm{N}_{\alpha_1,\cdots,\alpha_n}(f)$ の $\mathbb{Q}$ 上の既約因数分解を $G_1 \cdots G_r$ と表すとき、f の $\mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ 上の既約因数分解は

$$\gcd(f, G_1) \cdots \gcd(f, G_r)$$

で与えられる。

証明
f の $\mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ 上の任意の既約因子を h とすると、

$$h \mid \mathrm{N}(h), \quad h \mid f \ \Rightarrow \ \mathrm{N}(h) \mid \mathrm{N}(f)$$

となるので、h は $G_1, \cdots, G_r$ のどれか一つ、たとえば G_j、のみを割る: $h \mid \gcd(f, G_j)$。次に

$$g_i = \gcd(f, G_i)$$

に対し、g_i が $\mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ 上で既約であることを言う。

h と h' は $\mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ 上の異なる既約因子で $h \mid g_j$ かつ $h' \mid g_j$ と仮定する。$\mathrm{N}(h)$ は前定理より $\mathbb{Q}$ 上既約な多項式のべき乗だが、$\mathrm{N}(h) \mid \mathrm{N}(f)$ で $\mathrm{N}(f)$ が仮定より無平方だから、$\mathrm{N}(h)$ は $G_1, \cdots, G_r$ のどれかに等しい。$h \mid g_i$ の仮定より、それは G_i である。よって $\mathrm{N}(h) = G_i$。同様にして $\mathrm{N}(h') = G_i$ が言える。一方、$(hh') \mid f \ \Rightarrow \ \mathrm{N}(hh') \mid \mathrm{N}(f)$ であるから、${G_i}^2 \mid \mathrm{N}(f)$ となるが、これは $\mathrm{N}(f)$ が無平方の仮定に反する。従って g_i は $\mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ 上既約である。

補題 2
$\alpha_j \notin \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})$ かつ $f(x, \alpha_1, \cdots, \alpha_j) \in \mathbb{Q}(\alpha_1, \cdots, \alpha_j)[x]$ とする。$f(x, \alpha_1, \cdots, \alpha_j)$ が無平方 ならば、$\mathrm{N}_{\alpha_j}(f(x - s_j\alpha_j, \alpha_1, \cdots, \alpha_j))$ が 無平方でなくなる有理数値 s_j は有限個しかない。

証明
$\mathrm{N}_{\alpha_j}(f(x, \alpha_1, \cdots, \alpha_j))$ の無平方分解を ${g_1}{g_2}^2 \cdots {g_k}^k$ とし、

$$g(x, \alpha_1, \cdots, \alpha_{j-1}) = g_1 g_2 \cdots g_k$$

とおく。f は無平方なので、

$$f \mid g \ \Rightarrow \ \underset{\alpha_j}{\mathrm{N}}(f(x - s_j\alpha_j, \alpha_1, \cdots, \alpha_j)) \mid \underset{\alpha_j}{\mathrm{N}}(g(x - s_j\alpha_j, \alpha_1, \cdots, \alpha_{j-1})).$$

即ち、$\mathrm{N}_{\alpha_j}(f(x - s_j\alpha_j, \alpha_1, \cdots, \alpha_j))$ の重根はすべて $\mathrm{N}_{\alpha_j}(g(x - s_j\alpha_j, \alpha_1, \cdots, \alpha_{j-1}))$ の重根に含まれる。

g は無平方で $g \in \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})[x]$ であるから、問題は $\mathrm{N}_{\alpha_j}(g(x - s_j\alpha_j, \alpha_1, \cdots, \alpha_{j-1}))$ の無平方性に帰着される。

$$g = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_k)$$

とおくと、g が無平方ゆえ $\beta_i \neq \beta_j\ (i \neq j)$ となる。$g \in \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})[x]$ なので

$$\underset{\alpha_j}{\mathrm{N}}(g(x - s_j\alpha_j, \alpha_1, \cdots, \alpha_{j-1})) = \prod_{i=1}^{m_j}(x - s_j{\alpha_j}^{(i)} - \beta_1)(x - s_j{\alpha_j}^{(i)} - \beta_2)\cdots(x - s_j{\alpha_j}^{(i)} - \beta_k)$$

となる。これが無平方でなくなる為には、ある k, l, m, n が存在して

$$s_j\alpha_j^{(k)} + \beta_m = s_j\alpha_j^{(l)} + \beta_n \qquad (k, m) \neq (l, n)$$

が成立する事が必要である。ここで $\alpha_j^{(k)} \neq \alpha_j^{(l)}\ (k \neq l)$ に注意すると、上の条件は次のようになる。

$$s_j = \frac{\beta_n - \beta_m}{\alpha_j^{(k)} - \alpha_j^{(l)}} \qquad k \neq l.$$

これを満たす数値 s_j は有限個である。従ってこの s_j を有理数値に制限しても有限個である。

定理 3

$$\alpha_j \notin \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1}, \alpha_{j+1}, \cdots, \alpha_n)\ (j = 1, \cdots, n)$$

かつ

$$f(x, \alpha_1, \cdots, \alpha_n) \in \mathbb{Q}(\alpha_1, \cdots, \alpha_n)[x]$$

とする。$f(x, \alpha_1, \cdots, \alpha_n)$ が無平方ならば、

$$\underset{\alpha_1, \cdots, \alpha_n}{\mathrm{N}}(f(x - s_1\alpha_1 - \cdots - s_n\alpha_n, \alpha_1, \cdots, \alpha_n))$$

が無平方でなくなる有理数値 $s_i\ (i = 1, \cdots, n)$ は有限個しかない。

証明

$\mathrm{N}_{\alpha_n}(f(x - s_n\alpha_n, \alpha_1, \cdots, \alpha_n))$ が無平方でなくなる有理数値 s_n は前補題より有限個しかない。ここで、s_n を $\mathrm{N}_{\alpha_n}(f(x - s_n\alpha_n, \alpha_1, \cdots, \alpha_n))$ が無平方になるように選ぶと、再び前補題が適用できて、

$$\begin{aligned}&\underset{\alpha_{n-1}}{\mathrm{N}}\ \underset{\alpha_n}{\mathrm{N}}(f((x - s_{n-1}\alpha_{n-1}) - s_n\alpha_n, \alpha_1, \cdots, \alpha_n)))\\ &\quad = \underset{\alpha_{n-1}, \alpha_n}{\mathrm{N}}(f(x - s_{n-1}\alpha_{n-1} - s_n\alpha_n, \alpha_1, \cdots, \alpha_n))\end{aligned}$$

が無平方でなくなる有理数値 s_{n-1} は有限個しかないことが言える。これを繰り返せば、定理が導ける。

3. $\alpha_1, \cdots, \alpha_n$ に対する制限

$\mathbb{Q}$ に代数的数 $\alpha_1, \cdots, \alpha_n$ を順に添加していくとき、一般には α_i の最小多項式 D_i は $\mathbb{Q}(\alpha_1, \cdots, \alpha_{i-1})$ 上の多項式となる。これに対し、本稿では次の条件が成立する場合を扱う。

条件C： $i=1,\cdots,n$ に対し、α_i の最小多項式 D_i は $\mathbb{Q}$ 上の多項式で、
かつ $\alpha_i \notin \mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1},\alpha_{i+1},\cdots,\alpha_n)$ とする。

この制限は、数学的に見ればきわめてきついものだが、応用分野の多くの計算では満たされるものであり、実用的にはそれほどきついものではない (もちろん、条件Cを満たさない計算例はいくつもあるが)。

さて、最小多項式 D_i が $\mathbb{Q}$ 上の多項式でなくて $\mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})$ 上の多項式の場合、α_i に関するノルムは $\mathbb{Q}(\alpha_1,\cdots,\alpha_{i-1})$ 上で計算する必要がある。すなわち、$\mathrm{N}_{\alpha_1,\cdots,\alpha_i}(f)$ において、$\alpha_1,\cdots,\alpha_i$ の順序は決定的に重要で、勝手に変えることはできない。しかしながら、条件Cの下では $\alpha_1,\cdots,\alpha_i$ に関してノルムを取る順序は勝手に変えてよい。即ち、以下が成立する。

補題 3
$f \in \mathbb{Q}(\alpha_1,\cdots,\alpha_n)[x]$ とする。条件Cの下では

$$\underset{\alpha_j}{\mathrm{N}}(\underset{\alpha_i}{\mathrm{N}}(f)) = \underset{\alpha_i}{\mathrm{N}}(\underset{\alpha_j}{\mathrm{N}}(f)), \qquad i \neq j.$$

証明
自明である。

4. 条件Cの下での因数分解

$F(x) \in \mathbb{Q}[x]$ の $\mathbb{Q}(\alpha_1,\cdots,\alpha_n)$ 上での因数分解を Kronecker-Trager の方法で行うことを考える。まず、条件Cがない一般の場合を考える。この場合、ノルムはまず α_n に関して計算する必要があり、$\mathrm{N}_{\alpha_n}(F(x-s_n\alpha_n))$ を計算すると $\mathbb{Q}(\alpha_1,\cdots,\alpha_{n-1})$ 上の多項式が得られるから、問題は $\mathbb{Q}(\alpha_1,\cdots,\alpha_{n-1})$ 上の多項式の $\mathbb{Q}(\alpha_1,\cdots,\alpha_{n-1})$ 上での因数分解に帰着される。したがって、最終的に

$$\underset{\alpha_1,\cdots,\alpha_n}{\mathrm{N}}(F(x-s_1\alpha_1-\cdots-s_n\alpha_{n'}))$$

(これは $\mathbb{Q}$ 上の多項式) を $\mathbb{Q}$ 上で因数分解することになるが、このノルムは一般に高次の多項式とり、その次数は

$$\deg(F)\times m_1\times\cdots\times m_n$$

である。この場合、$s_1\alpha_1+\cdots+s_n\alpha_n$ は $\mathbb{Q}(\alpha_1,\cdots,\alpha_n)$ の原始元ゆえ、この方法は1個の原始元を添加する方法と本質的には同じである。

次に、条件Cがある場合を考える。この場合、ノルムは $\alpha_1,\cdots,\alpha_n$ のそれぞれについて勝手な順序でとることができ、しかも $\mathrm{N}_{\alpha_i}(F(x-s_i\alpha_i))$ は $\mathbb{Q}$ 上の多項式となる。したがって、まず $\mathbb{Q}(\alpha_1)$ 上で $F(x)$ を因数分解し、その各因子を $\mathbb{Q}(\alpha_1,\alpha_2)$ 上で因数分解し、$\cdots$、というように因数分解を分割して行うことができる (ある種の divide-and-conquer である)。さらに、Kronecker-Trager の算法を素直に適用する場合に比べて、いくつかのステップを省略できる。そのことを $\mathbb{Q}(\alpha_1,\alpha_2)$ 上での因数分解を例にとって説明しよう。

$\mathbb{Q}(\alpha_1,\alpha_2)$ 上での Kronecker-Trager's algorithm。

因数分解すべき多項式 $F(x)\in\mathbb{Q}[x]$、　F は無平方で $\mathbb{Q}$ 上原始的とする。
ただし、拡大体 $\mathbb{Q}(\alpha_1,\alpha_2)$ は条件Cを満たす。

———(i) まず、 $\mathbb{Q}(\alpha_1)$ 上で F を因数分解する ———

$\mathrm{N}_{\alpha_1}(F(x-s_1\alpha_1))$ が無平方となるよう、有理数 s_1 を選び、

$$f(x,\alpha_1)=F(x-s_1\alpha_1)$$

とおく。

次に、 $\mathrm{N}_{\alpha_1}(f(x,\alpha_1))$ を $\mathbb{Q}$ 上で因数分解する:

$$\underset{\alpha_1}{\mathrm{N}}(f(x,\alpha_1))=G_{1,1}(x)\cdots G_{1,r_1}(x). \tag{\#}$$

上記右辺の各因子 $G_{1,j}$ に対し、 $f(x,\alpha_1)$ との GCD を計算する:

$$\gcd(f(x,\alpha_1),\ G_{1,j}(x))=g_{1,j}(x,\alpha_1)\qquad(j=1,\cdots,r_1). \tag{1}$$

すると、 $f(x,\alpha_1)$ の $\mathbb{Q}(\alpha_1)$ 上の因数分解が以下のように得られる。

$$g_{1,1}(x,\alpha_1)\cdot\cdots\cdot g_{1,r_1}(x,\alpha_1).$$

———(ii) 次に、 $\mathbb{Q}(\alpha_1,\alpha_2)$ 上で $g_{1,j}$ を因数分解する ———

上記 (i) で得られた各既約因子 $g_{1,i}$ に関して以下を実行する。

$\mathrm{N}_{\alpha_1}\mathrm{N}_{\alpha_2}(g_{1,i}(x-s_2\alpha_2,\alpha_1))$ が無平方となるよう、有理数 s_2 を選ぶ。
次に $\mathrm{N}_{\alpha_1}\mathrm{N}_{\alpha_2}(g_{1,i}(x-s_2\alpha_2,\ \alpha_1))$ を $\mathbb{Q}$ 上で因数分解する:

$$\underset{\alpha_1}{\mathrm{N}}\,\underset{\alpha_2}{\mathrm{N}}(g_{1,i}(x-s_2\alpha_2,\ \alpha_1))=G^{(i)}_{2,1}(x)\cdots G^{(i)}_{2,r_2^{(i)}}(x). \tag{2}$$

上記右辺の各因子 $G^{(i)}_{2,k}$ と $g_{1,i}(x-s_2\alpha_2,\alpha_1)$ との GCD を計算する：

$$\gcd(g_{1,i}(x-s_2\alpha_2,\alpha_1),G^{(i)}_{2,k}(x))=g^{(i)}_{2,k}(x,\alpha_1,\alpha_2)\qquad(k=1,\cdots,r_2^{(i)}). \tag{\#\#}$$

すると、 $F(x)$ の $\mathbb{Q}(\alpha_1,\alpha_2)$ 上での因数分解が次のように得られる。

$$\prod_{i=1}^{r_1}\prod_{j=1}^{r_2^{(i)}}g^{(i)}_{2,j}(x+s_1\alpha_1+s_2\alpha_2,\alpha_1,\alpha_2).$$

見て分るように、このアルゴリズムはまず、$F(x)$ を $\mathbb{Q}(\alpha_1)$ 上で因数分解し、次にこの各既約因子を $\mathbb{Q}(\alpha_1,\alpha_2)$ 上で因数分解している。したがって、因数分解を分割して行なっている。$F(x)$ が $\mathbb{Q}(\alpha_1)$ 上で常に複数の因子に分解できるとは限らないが、分解できる場合には、大きな次数の多項式を一度に因数分解する普通の方法よりもはるかに有利である。

上記のアルゴリズムはさらに、以下のように効率化できる。上のアルゴリズムで (2) 式に注目する。条件Cの下では $\mathrm{N}_{\alpha_1}\mathrm{N}_{\alpha_2}(g_{1,i}) = \mathrm{N}_{\alpha_2}\mathrm{N}_{\alpha_1}(g_{1,i})$ であるから、

$$\begin{aligned}\underset{\alpha_1}{\mathrm{N}}\underset{\alpha_2}{\mathrm{N}}(g_{1,i}(x-s_2\alpha_2,\alpha_1)) &= \underset{\alpha_2}{\mathrm{N}}\underset{\alpha_1}{\mathrm{N}}(g_{1,i}(x-s_2\alpha_2,\alpha_1))\\ &= \underset{\alpha_2}{\mathrm{N}}(G_{1,i}(x-s_2\alpha_2))\end{aligned}$$

となる。したがって、(#) から (##) までの過程が省略でき、

$$\begin{aligned}&\underset{\alpha_1,\alpha_2}{\mathrm{N}}(F(x-s_1\alpha_1-s_2\alpha_2))\\ &\quad=\underset{\alpha_2}{\mathrm{N}}\underset{\alpha_1}{\mathrm{N}}(F(x-s_1\alpha_1-s_2\alpha_2))\\ &=\underset{\alpha_2}{\mathrm{N}}\left(\prod_{i=1}^{r_1}G_{1,i}(x-s_2\alpha_2)\right)\qquad(\mathrm{N}_{\alpha_1}(F(x-s_1\alpha_1))\text{ の因数分解})\\ &=\prod_{i=1}^{r_1}\underset{\alpha_2}{\mathrm{N}}(G_{1,i}(x-s_2\alpha_2))\\ &=\prod_{i=1}^{r_1}\prod_{j=1}^{r_2^{(i)}}G_{2,j}^{(i)}(x)\qquad(\mathrm{N}_{\alpha_2}(G_{1,i}(x-s_2\alpha_2))\text{ の因数分解})\end{aligned}$$

となる。そして、$F(x-s_1\alpha_1-s_2\alpha_2)$ の $\mathbb{Q}(\alpha_1,\alpha_2)$ 上の因数分解が以下のように求まることが分る。

$$\prod_{i=1}^{r_1}\prod_{j=1}^{r_2^{(i)}}\gcd(F(x-s_1\alpha_1-s_2\alpha_2),G_{2,j}^{(i)}).$$

この方法は、$\mathbb{Q}(\alpha_1,\alpha_2)$ から $\mathbb{Q}(\alpha_1,\cdots,\alpha_n)$ へ容易に延長できる。

参 考 文 献

[1] van der Waerden, 現代代数学 1 , §42, 東京図書.

[2] B. M. Trager, Algebraic Factoring and Rational Function Integration, Proc. SYMSAC, pp. 219-226, 1976.